Deutscher Bundestag **Drucksache 19/9456**
19. Wahlperiode 16.04.2019

Kleine Anfrage

der Abgeordneten Renate Künast, Tabea Rößner, Dr. Konstantin von Notz, Dieter Janecek, Dr. Anna Christmann, Luise Amtsberg, Dr. Danyal Bayaz, Canan Bayram, Dr. Franziska Brantner, Ekin Deligöz, Katharina Dröge, Britta Haßelmann, Katja Keul, Sven-Christian Kindler, Christian Kühn (Tübingen), Monika Lazar, Sven Lehmann, Steffi Lemke, Irene Mihalic, Beate Müller-Gemmeke, Filiz Polat, Dr. Manuela Rottmann, Stefan Schmidt und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Datenschutz im Kinderzimmer – Digitales und vernetztes Spielzeug

„Intelligentes“, mit dem Internet verbundenes Spielzeug, sogenannte Smart Toys wie digitalisierte Roboter, Uhren, Teddybären oder Puppen sind mittlerweile weit verbreitet – auch auf dem bundesdeutschen Markt. Diese technischen Geräte können zum Teil sensorgesteuert selbständig auf Handlungen von Kindern reagieren.

Diese technischen Geräte werfen zahlreiche, ganz unterschiedlich gelagerte Rechtsfragen in den verschiedensten Rechtsbereichen auf, beispielsweise im Recht der IT-Sicherheit, im Verbraucherschutz- und Datenschutzrecht sowie im Haftungsrecht (vgl. etwa Hornung, VuR 2018, S. 41). Sogenannte Smart Toys zählen zu den Geräten des „Internet of Things“ (IoT) und teilen insoweit zahlreiche mit der IKT-Entwicklung sowie u. a. der Thematik „Smart Homes“ verbundene Fragen. Aufgrund der besonderen Verletzlichkeit von Kindern und der spezifischen grundrechtlichen Schutzanforderungen für Kinder stellen sich darüber hinaus noch deutlich weitergehende Fragen.

Als mit dem Internet verbundene Systeme können internetgestützte Sprachassistenzsysteme in gewissem Umfang Fragen der Kinder beantworten, manche ermöglichen ein ständiges Tracking des Aufenthaltsortes von Kindern. Zahlreiche Geräte erfassen alle Geräusche, Stimmen und Unterhaltungen in ihrer Umgebung, speichern diese und senden sie zur Analyse an zentrale, oft im Ausland liegende Server. Inwieweit es zur weiteren Verarbeitung und Auswertungen der erfassten Kommunikationen kommt, bleibt oftmals unklar.

Wiederholt wurden gravierende Sicherheitslücken bei entsprechenden Geräten festgestellt, die sich mit geringstem Aufwand von außen übernehmen und zu Missbrauchszwecken wie z. B. Identitätsdiebstahl einsetzen ließen (vgl. etwa Marktwächter VZBV NRW, www.marktwaechter.de/pressemeldung/kein-kinderspiel-vernetztes-spielzeug-birgt-risiken).

Klein- und Kleinstkinder werden mit digitalem Spielzeug ab den ersten Monaten ihres Lebens der Möglichkeit ständiger Erfassung und Beobachtung, auch durch unbefugte Dritte, unterworfen. Manipulative Zugriffe von außen im besonders geschützten Wohn- und Lebensbereich können das Recht auf Privatheit und Unverletzlichkeit der Wohnung aushöhlen. Von ihrer IT-Sicherheit dürftig bis überhaupt nicht abgesicherte Massenprodukte können von außen leicht übernommen

werden: damit kann die Ausspähung und Manipulation des privaten Wohnumfelds zum Kinderspiel werden. Je nach Produkt können nach Ansicht der Fragesteller Unbefugte über die Geräte Kommunikation von außen mit den Kindern aufnehmen. Auch unbeteiligte Dritte können dabei in ihren Grundrechten verletzt werden. Damit sind auch grundlegende Fragen des Rechts auf Integrität und Unverletzlichkeit informationstechnischer Systeme aufgeworfen.

Die Risiken dieser digitalisierten Spielzeuge für die Rechte aller davon Betroffenen, insbesondere aber der Kinder, sind zahlreich und gravierend. Den Staat trifft mit Blick auf die Persönlichkeitsentwicklung von Kindern und deren Persönlichkeitsrechte, aber auch mit Blick auf die Voraussetzungen einer demokratischen und rechtsstaatlich verfassten Gesellschaft eine umfassende Schutzpflicht.

Der Deutsche Bundestag hat sich bereits im März 2016 erstmalig aufgrund einer Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN mit sogenannten Smart Toys und speziell der Puppe Cayla befasst (vgl. Bundestagsdrucksache 18/8317).

Spätestens mit dem Anfang 2017 nach § 90 des Telekommunikationsgesetzes ausgesprochenen Verbot der Spielzeugpuppe Cayla als unbefugte Sendeanlage sowie dem Verbot weiterer Produkte aus diesem Bereich durch die Bundesnetzagentur sind die Risiken „intelligenter" Spielzeuge einer breiteren Öffentlichkeit bekannt geworden.

Die Digitalisierung macht vor den Kindern aller Altersgruppen insgesamt nicht halt, im Gegenteil. Kinder haben oftmals Zugang zu und nutzen in rasant zunehmendem Umfang Smartphones und andere digitale Geräte wie z. B. digitale Sprachassistenzsysteme. Ob und inwieweit die Bundesregierung sich zu dieser Entwicklung konstruktiv und problemangemessen verhält und ihrer Schutzverantwortung angemessen gerecht wird, ist insoweit von großer gesellschaftlicher Bedeutung.

Die Bundesregierung will sich zwar nach eigenen Angaben dafür einsetzen, auf Basis der Aktualisierung des EU Cybersecurity Acts (CSA) verpflichtende Mindestsicherheitsstandards für loT-Geräte zu etablieren (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN zur Sicherheit und Konformität von loT-Geräten, Bundestagsdrucksache 19/9132, S. 3). Im aktuellen Trilog-Ergebnis zum CSA (vgl. http://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf) werden mit Unterstützung der Bundesregierung nun allerdings nur freiwillige Zertifizierungen in Eigenregie der Hersteller nach vertikalen Zertifikationsschemata und mit selbst verliehenen Sicherheitssiegeln in Aussicht gestellt ohne Angabe von Sanktionsmaßnahmen bei Verstößen oder gar Haftungsregeln. Auch die Frage, inwieweit es im Zuge der Vorlage des „IT-Sicherheitsgesetzes 2.0" der Bundesregierung zu verpflichtenden Mindeststandards und neuen Haftungsregelungen kommt, ist derzeit noch offen.

Wir fragen daher die Bundesregierung:

1. Verfügen die Bundesregierung und die ihr nachgeordneten Behörden inzwischen über aktualisierte Ergebnisse der Marktbeobachtung, die ihr eine Einschätzung der zahlreichen und zum Teil sehr unterschiedlich gelagerten Risiken der den deutschen Markt erreichenden Smart Toys erlauben, und wenn ja, wie lauten diese, und wenn nein, was unternimmt die Bundesregierung, um ein entsprechend differenziertes Bild zu erhalten (bitte nach Behörden aufschlüsseln)?
2. Fällt nach Auffassung der Bundesregierung die Sicherheit von digitalem Spielzeug in die Zuständigkeit der Marktüberwachung nach dem Produktsicherheitsgesetz?
3. Welche konkreten Positionen hat die Bundesregierung mit Blick auf die besonderen datenschutzrechtlichen Risiken von vernetzten „Smart Toys“ und anderen IoT-Geräten im Zusammenhang mit den Verhandlungen zur E-Privacy-Verordnung und der Aushandlung des Cybersecurity Acts vertreten, um ein sachgerechtes hohes Schutzniveau der Verbraucherinnen und Verbraucher sicherzustellen?
4. Was hat die Bundesregierung bzw. speziell das federführende Bundesministerium für Wirtschaft und Energie konkret bewogen, im Rahmen ihrer Anpassung bundesdeutscher Rechtsvorschriften an die EU-Datenschutz-Grundverordnung (DSGVO) ihren bereits aufgenommenen Referentenentwurf zur Anpassung des Telekommunikationsgesetzes (TKG), nicht weiterzuverfolgen und auch im Rahmen der Vierten Änderung des Telekommunikationsgesetzes nicht für die erforderliche Klarheit hinsichtlich der geltenden Vorschriften zu sorgen?
5. Teilt die Bundesregierung die Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Stellungnahme gegenüber dem Innenausschuss des Deutschen Bundestages 19(4)151 vom 26. Oktober 2018), wonach durch die Nichtanpassung der Rechtsvorschriften insbesondere des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) erhebliche Rechtsunsicherheit hinsichtlich des anzuwendenden Rechts entstanden ist, welche auch den notwendigen Vollzug der Bestimmungen nachteilig beeinträchtigen könnte, und wenn nein, warum nicht?
6. Inwiefern teilt die Bundesregierung die Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (siehe ebenfalls die in Frage 4 angeführte Stellungnahme), wonach die Bundesnetzagentur (BNetzA) nicht den Anforderungen entspricht, die das europäische Recht an die Unabhängigkeit und Weisungsfreiheit der Datenschutzvorschriften kontrollierenden Stellen aufstellt (Artikel 8 Absatz 3 der Charta der Grundrechte der Europäischen Union; Artikel 16 Absatz 2 Satz 2 des Vertrags über die Arbeitsweise der Europäischen Union sowie dazu ergangene die eindeutige Rechtsprechung des Gerichtshofs der Europäischen Union), und wenn sie diese teilt, wann wird die Bundesregierung hier die Verhältnisse den entsprechenden Anforderungen anpassen?
7. Teilt die Bundesregierung die Auffassung, dass der unabhängige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vollständig mit der Aufgabe der Aufsicht über die Einhaltung der Datenschutzbestimmungen im Bereich der Telekommunikationsunternehmen betraut werden sollte und dazu gesetzlich die bisherigen Sanktionsmöglichkeiten der Bundesnetzagentur eingeräumt bekommen sollte, und wenn nein, warum nicht?

8. Teilt die Bundesregierung die Auffassung, dass die bisherige Beschränkung des Produktsicherheitsrechts auf das Schutzgut der körperlichen Integrität weder die besondere Gefahrenlage vernetzter Spielzeuge und anderer IoT-Geräte mit ihrer Vielzahl eingebauter Schwachstellen, noch die berechtigten Schutzerwartungen der Nutzerinnen und Nutzer abzubilden in der Lage ist (vgl. etwa Bäumerich, DVBl. 2019, S. 219, 224), und empfiehlt sich vor diesem Hintergrund ein zumindest bereichsbezogenes nationales oder europäisches Produktsicherheitsrecht für Software oder zumindest für sogenannte Smart Toys und wenn nein, warum nicht?
9. Sieht die Bundesregierung angesichts der bereits bekannt gewordenen Probleme bei vernetztem Spielzeug und anderen IoT-Geräten die Notwendigkeit, den Sicherheitsbegriff in der europäischen Spielzeugrichtlinie auszuweiten, so dass auch Gesundheit, IT-Sicherheit und Datenschutz zur Anforderung der Spielzeugsicherheit werden, und wenn nein, warum nicht?
10. Wirkt die Bundesregierung darauf hin oder hat sie bereits, wenn ja in welchem konkreten Kontext, darauf hingewirkt, dass die EU-Kommission eine Überarbeitung der Spielzeugrichtlinie mit dem Ziel der Einbeziehung von vernetzten digitalen Spielzeugen und anderen IoT-Geräten hinsichtlich typischer Risiken vornimmt, und wenn nein, warum nicht?
11. Inwiefern wirkt die Bundesregierung auf europäischer Ebene auf eine verpflichtende Drittzertifizierung für Spielzeug und andere IoT-Geräte hin, die neben anderen Sicherheitsaspekten auch IT-Sicherheits- und Datenschutzrisiken berücksichtigt, und wenn nein, warum nicht?
12. Werden festgestellte Verstöße wie im Fall der Spielzeugpuppe „Cayla“ oder festgestellte Datenschutz- und IT-Sicherheitsmängel von den zuständigen Behörden an das europäische Schnellwarnnetzwerk RAPEX weitergegeben, und wenn ja, in wie vielen Fällen in den letzten drei Jahren (bitte konkret auflisten), und wenn nein, warum nicht?
13. Teilt die Bundesregierung den von der britischen Regierung für IoT-Produkte allgemein formulierten Anforderungskatalog (vgl. EPIC-Stellungnahme, S. 4, https://epic.org/comments/EPIC-Comments-EU-Toy-Safety-Directive.pdf), und wenn nein, welche vergleichbaren Sicherheits-Anforderungen sieht sie im Falle von „Smart Toys“ und anderen IoT-Geräten als einschlägig an?
14. Wie bewertet die Bundesregierung das Vorgehen der Bundesnetzagentur (BNetzA) in Fällen, bei denen die Positionsdaten und weitere Informationen von mehreren Tausend Kindern abgegriffen werden können, aber offenbar keine systematische Prüfung der Produktpaletten und Intervention seitens der Bundesnetzagentur erfolgte (vgl. http://0x0000dead.de/Watchgate_TROOPERS2019.pdf)?
15. Hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits oder plant es eigene Untersuchungen im Bereich der „Smart Toys“ oder anderer IoT-Produkte mit dem Ziel der Verbraucherunterstützung und Verbrauchersicherheit, und wenn nein, warum nicht?
16. Wie viele Beschäftigte der Bundesnetzagentur sind mit der Sichtung und Kontrolle der in ihren Zuständigkeitsbereich fallenden „intelligenten“ Spielzeugprodukte und anderer IoT-Geräte befasst, und hält die Bundesregierung diese Ausstattung mit Blick auf Quantität und Qualität der Herausforderung für angemessen?

17. Welchen Beitrag wird die Bundesregierung dafür leisten, dass auch die Datenschutzbehörden des Bundes und der Länder ihren gesetzlichen Verpflichtungen durch sachgerechte Ausstattung und finanzielle Ressourcen nachkommen können, die besonderen Risiken vernetzter Spielzeuge und vernetzter Produkte zu adressieren und die Durchsetzung des Datenschutzrechts zu gewährleisten?
18. Wie bewertet die Bundesregierung die Gefahr, dass unsichere „smarte“ Spielzeuge und andere IoT-Geräte zu Botnetzen verbunden werden, die wiederum für IT-Angriffe verwendet werden?
19. Wie bewertet die Bundesregierung die Gefahr, dass unsichere „smarte“ Spielzeuge und andere IoT-Geräte, die mit einer Videofunktion versehen sind, von Dritten übernommen werden und entsprechende Bildaufzeichnungen für verschiedene (kriminelle) Zwecke missbraucht werden können?
20. Wie bewertet die Bundesregierung Gefahren, die dadurch entstehen, dass Kommunikationen über „smartes“ Spielzeug und andere IoT-Geräte auch auf Servern in Ländern gespeichert werden, in denen entsprechende gesetzliche Regelungen Sicherheitsbehörden und Nachrichtendiensten weitreichende Zugriffsrechte gewähren, beispielsweise in China und den USA?
21. Wie bewertet die Bundesregierung das aktuelle Trilog-Ergebnis zum Cybersecurity Act (CSA) (vgl. http://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf) auch vor dem Hintergrund der eigenen Ankündigung, sich dafür einsetzen zu wollen, verpflichtende Mindestsicherheitsstandards für loT-Geräte zu etablieren (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN zur Sicherheit und Konformität von loT-Geräten, Bundestagsdrucksache 19/9132, S. 3)?
22. Hält die Bundesregierung freiwillige Zertifizierungen in Eigenregie der Hersteller nach vertikalen Zertifikationsschemata und mit selbst verliehenen Sicherheitssiegeln ohne tatsächliche Sanktionsmaßnahmen bei Verstößen oder gar Haftungsregeln für tatsächlich ausreichend?

    Wenn ja, wie erklärt sich der Sinneswandel (vgl. ebd.)?
23. Wird die Bundesregierung im Zuge der Vorlage des „IT-Sicherheitsgesetzes 2.0“ neue, verpflichtende Mindeststandards und Haftungsregelungen vorlegen?

    Falls ja, wie sehen diese konkret aus?

    Falls nein, warum nicht?
24. Inwiefern ist es nach Kenntnis der Bundesregierung deutschen Ermittlungsbehörden im Rahmen von Strafverfahren möglich, auf die aus intelligenten Spielzeugprodukten übertragenen (und auf Servern gespeicherten) Daten zuzugreifen, und wie viele solche Fälle sind der Bundesregierung bekannt (bitte nach Rechtsgrundlage aufschlüsseln)?

Berlin, den 9. April 2019

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333